How to Implement Cyber Insurance

Cyber Insurance for Medium/large-sized Healthcare Organizations

HHS 405(d)
Aligning Health Care
Industry Security Approaches

What is Cyber Insurance?

Cyber Insurance is one option that can help protect your business against losses resulting from a cyber attack. Cyber insurance is an on-going partnership between you and your insurance company, used to continually improve your organization's security and ensure that needed protections are present and available in the event of a cyber attack. Working in partnership with your insurance company can help augment your organization's practices to address security requirements, while effectively managing your premium costs.

Why is it important?

Due to the increase in targeted attacks on the healthcare sector, having added protection can ensure you will not have to shut your doors if you become the victim of a cyber attack. Cyber insurance can help protect your organization from excessive costs that might can occur in the event of a cyber attack. It can prevent your organization from potentially going out of business due to a successful attack.

How will this keep my organization safe?

If your organization becomes the victim of a cyber attack cyber insurance can provide your organization with access to third-party breach specialists including forensics, independent legal counsel working on your behalf, and possible reimbursement of loss of business coverage or revenue.

Threats Cyber Insurance Mitigates:

- Social engineering
- Ransomware attack
- Loss or theft of equipment or data
- Insider, accidental or malicious data loss
- Attacks against network connected medical devices

Implementation Tips:

Secure a cyber insurance policy that provides ransomware protections. The healthcare and public health sector is increasingly targeted by ransomware attacks due to its valuable Public Health Information. The costs to bring systems back online and recover possible data loss due to an attack can cause a great financial impediment to your organization. Having cyber- insurance could help lessen the impact and provide needed resources.

Inquire if your policy will offer a breach hotline. Ensure that it is available every day of the year at all times to ensure that your organization can remain in contact with your incident response team members.

Consider whether your policy can defend you in a lawsuit or regulatory investigation. Also called a "duty to defend". Having access to legal representation after a breach can significantly help manage the incident as well as consult on regulatory expectations.

Inquire whether your policy require you to use specific vendors for Incident Response. Ensure that when you acquire your cyber insurance policy that you become familiar with the stakeholders that your policy utilizes for incident response. Therefore, you will be in alignment with your policy requirements.

To learn more about how you can protect your patients from cyber threats check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication. Check out the available resources 405(d) has to offer by visiting our website at 405d.hhs.gov and our social media pages: **@ask405d** *on Facebook, X, LinkedIn and Instagram!*